Alert: Cyberattacks by MirrorFace
(Provisional Translation)

The National Police Agency (NPA) and the National center of Incident readiness and Strategy for Cybersecurity (NISC) have assessed that the following cyberattack campaigns against organizations, businesses, and individuals in Japan from approximately 2019 to the present have been conducted by cyber threat actors called “MirrorFace” (also known as “Earth Kasha”).

1. Between 2019 and 2023, NPA and NISC have observed cyberattacks that attempted to steal information from individuals and organizations, primarily related to think tanks, government (including retirees), politicians, and mass media in Japan, by sending them emails with malicious attachments. (Hereinafter referred to as “Attack Campaign A”).

2. NPA and NISC have confirmed cyberattacks since around 2023, which exploit software vulnerabilities in the Internet-connected devices to infiltrate into target networks. The main targets were Japan's semiconductors, manufacturing, telecommunications, academia, and aerospace sectors. (Hereinafter referred to as “Attack Campaign B”).

3. Since around June 2024, NPA and NISC have confirmed cyberattacks that attempt to steal information from individuals and organizations, mainly related to academia, think tanks, politicians, and mass media in Japan, by sending them emails containing links to download malware. (Hereinafter referred to as “Attack Campaign C”).

Both Attack Campaigns A and C are targeted e-mail attacks, but MirrorFace employs different types of malware and infection methods. . While malware called LODEINFO was used in Attack Campaign A, and the infection mainly started from opening an attached file, the NPA and the NISC have confirmed that malware called ANEL was used in Attack Campaign C, and the infection mainly started from a link on the e-mail. After the intrusion, it has also been confirmed that Attack Campaign C exploited Visual Studio Code (VS Code), in addition to the Windows Sandbox exploit that had been confirmed throughout each campaign.

As a result of analysis of the attack targets, tactics, techniques, and procedures (TTPs) , and attack infrastructure, etc., which were identified through investigations by the National Cyber Department of the NPA, the Tokyo Metropolitan Police Department, and other prefectural police, these campaigns by MirrorFace have been assessed as a series of organized cyberattack activities with suspected Chinese involvement, mainly aimed at information theft related to national security and advanced technologies in Japan.

This alert, disclosing the methods employed by MirrorFace, aims to raise awareness among target organizations, businesses and individuals about the growing threats in cyberspace, and encourages to take appropriate cyber security measures in order to prevent and limit cyber damage.

In addition, if you recognize any suspicious activity on your devices or any suspicious communication in your network, please promptly provide the information to the competent ministries and agencies, the police, the NISC, or other cybersecurity-related organizations.

For more detail information, visit our Japanese version website.